

-6-

REMARKS

The Examiner has again rejected Claims 1-4, 6, 7, 9, 11-14, 16, 17 and 19-21 under 35 U.S.C. 102(e) as being anticipated by Webber, Jr. Applicant respectfully disagrees with such rejection, especially in view of the amendments made previously.

In particular, the Examiner has dismissed applicant's claim amendments by stating that the claimed "security-related" interaction is met by the following excerpt from Webber.

"An additional level of security may be provided by only activating contracts which are marked with a special authorization encryption or signature. Modification of any one element in the contract and CAP without simultaneously making the same change at all levels would immediately become evident and should readily be detected. Since the contracts are linked together, reconciliation, verification and authentication can be performed by comparing transactional data at one level for one party with the corresponding transaction for all parties at all levels. Alternatively, the CAP can operate as an exception system, by identifying deviations, rather than reviewing all transactional details." (col. 15, lines 13-24)

While such excerpt shows "security-related" activity, it fails to meet the specific context in which applicant's "security-related" interaction is claimed. As emphasized in the previous response, applicant does not merely claim "security-related" activity, but rather "governing a security-related interaction between a plurality of components of the system utilizing the criteria of the contract, the components including an intrusion detection module which is subject to the governing."

It appears that the Examiner continues to fail to consider the full weight of applicant's claim limitations (including, in particular, the functional limitations and their relation to the claimed intrusion detection module). Webber's activation of contracts based on special authorization encryption or signatures simply does not meet applicant's claimed "governing a security-related interaction between a

NAI1P002/00.056.01

- 6 -

-7-

plurality of components" "including an intrusion detection module which is subject to the governing" "utilizing the criteria of the contract" (emphasis added).

Thus, it appears that the Examiner is trying to stretch Webber's teachings of a security technique for protecting against contract fraud and detecting the authenticity of the contracts themselves, to meet applicant's claimed invention involving governing an intrusion detection module based on a contract. This is improper, as this attempt does not anticipate each element of applicant's claimed invention (even in their broadest sense). Just by way of example, Webber fails to even suggest an "intrusion detection module," let alone a contract governed-intrusion detection module.

There is simply no teaching, disclosure and/or suggestion in Webber of any sort of governing of a security-related interaction involving an intrusion detection module utilizing the criteria of a contract.

Further emphasizing this distinction (and overlooked by the Examiner) is applicant's claimed "governing a security-related interaction between ... a plurality of intrusion detection modules, and at least one firewall which are subject to the governing" (emphasis added). See previously amended Claim 21.

Again, the contracts of Webber govern *commercial* transactions among parties. The only mention of any security-related components is in passing, and simply does not meet applicant's claimed contract-governed security-related interaction among a plurality of intrusion detection modules, and at least one firewall.

In the latest action, the Examiner relies on the following excerpts to make a 102(e) prior art showing of the foregoing limitations:

"In accordance with one embodiment of the invention, there is provided a method for digital automation of supply chains. In a computerized system, at least one non-ratified contract is generated for a transaction in one supply chain of the supply

-8-

chains, wherein the non-ratified contract has a plurality of terms. The contract is ratified and stored as a ratified contract in a database in the computerized system. If a term of the plurality of terms in the ratified contract indicates that at least one next contract is necessary for a next transaction in the supply chain, the above steps are repeated for the at least one next contract, and links between the ratified contract and the next contract are stored in the database." (col. 5, lines 4-15)

"In the preferred embodiment, the CAP and computing module utilize available secure socket layer protocols and public key encryption technology, such as that available from RSA Data security. A commercially available firewall advantageously protects and verifies a customer identifier associated with the customer, a bank identifier associated with the bank, and passwords." (col. 8, lines 59-65)

"The CAP is advantageously designed in a modular fashion so that each function is a separate independent subsystem. These independent subsystems include: security and firewalls, auditing, inventory management, management reporting, accounting, statistical logging and reporting, shipping options, distribution options, purchasing services, delivery/shipping schedules, integration of shipping with suppliers." (col. 14, lines 4-11)

Applicant asserts that the Examiner can not simply point to a general description of "firewalls" in a system with "contracts ... generated for a transaction in one supply chain of the supply chains," (see Claim 1 of Webber, for example) and then erroneously infer that such a system suggests that the contracts govern a security-related interaction between an intrusion detection module and a plurality of firewalls, in the context of the remaining claim limitations of applicant's invention. To do so would require one to ignore or dismiss applicant's claim limitations, which would be improper.

An indication of allowable subject matter or a specific showing in the prior art of a contract-governed interaction among an "intrusion detection module" and multiple "firewalls" in the context of the remaining claim limitations is respectfully requested.

The Examiner has again rejected Claims 5 and 15 under 35 U.S.C. 103(a) as being unpatentable over Webber, Jr., as applied above, and further in view of Bigus.

NAIIP002/00.056.01

- 8 -

-9-

By virtue of the dependence of such claims on the independent claims discussed hereinabove, such claims are deemed allowable along with the remaining pending dependent claims.

An allowance is respectfully requested.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. If any fees are due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NA11P002/00.056.01).

Respectfully submitted,

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172
Telephone: (408) 505-5100

NA11P002/00.056.01

-9-